Abstract

Methods and systems for firewall/data protection that filters data packets in real time and without packet buffering are disclosed. A data packet filtering hub, which may be implemented as part of a switch or router, receives a packet on one link, reshapes the electrical signal, and transmits it to one or more other links. During this process, a number of filters checks are performed in parallel, resulting in a decision about whether each packet should or should not be invalidated by the time that the last bit is transmitted. To execute this task, the filtering hub performs rules-based filtering on several levels simultaneously, preferably with a programmable logic or other hardware device. Various methods for packet filtering in real time and without buffering with programmable logic are disclosed. The system may include constituent elements of a stateful packet filtering hub, such as microprocessors, controllers, and integrated circuits. The system may be reset, enabled, disabled, configured, and/or reconfigured with toggles or other physical switches. Audio and visual feedback may be provided regarding the operation and status of the system.